HITACHI
Inspire the Next

JOB DESCRIPTION

Title of Position	Cyber Threat Hunter
Department	MSS
Immediate Supervisor	VP, Managed Security Services
Location	Blainville

Summary of the Role:

The *Cyber Threat Hunter* will be responsible for participating in threat actor-based investigations to detect, disrupt and eradicate the presence of threat actors from enterprise networks. To meet this goal, you will utilize the latest in cyber security technology and Cyber Threat Intelligence to support Hitachi Systems Security Inc. customers with proactive Computer Network Defense protection.

Primary Responsibilities:

- Hunt for and identify threat actor groups based on their known techniques, tactics, procedures (TTPs), tools and infrastructure.
- Identify and track new tactics, techniques, and procedures (TTPs) associated with known threat actors to enhance our cyber threat intelligence database.
- Capture intelligence on threat actor TTPs and develop countermeasures in response to threat actors.
- Conduct Open Source cyber threat intelligence research to identify threat actor motivations, capabilities, and intentions.
- Monitoring and analysis of network traffic and security alerts, responding to potential threats and vulnerabilities.
- Investigation of intrusion attempts and performing in-depth reverse engineering analysis of exploits.
- Provide network intrusion detection expertise to support timely and effective decision on when to declare an incident.
- Perform initial triage on security events that are populated in Hitachi's Security Information and Event Management (SIEM) system.
- Analyze a variety of network and endpoint-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine the correct remediation actions and escalation paths for each incident.
- Independently follow procedures to contain, analyze, and eradicate malicious activity.
- Document all activities during an incident and provide leadership with status updates during the life cycle of the incident.

- Develop advanced queries and alerts to detect adversary actions.
- Provide thoroughly vetted intelligence products on emerging cyber threats, indicators of compromise and trend analysis.
- Create a final incident report detailing the events of the incident.
- Provide information regarding intrusion events, security incidents, and other threat indications and warning information to US government agencies.
- Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC operations.

Qualifications Required:

- Minimum of two (2) years of direct experience in an IT Security, Incident Response or Security Analyst role within the last 4 years.
- Industry recognized professional certification such as GCFA, GREM, GCIH, CISSP
- Experience with or current understanding of Cyber intelligence processes and systems.
- Direct experience with Malware and Fusion analysis techniques and methodologies.
- Scripting skills (e.g., PowerShell, Python, shell scripting)
- Experience with cyber advanced persistent threats, actors, infrastructure, and TTPs.
- Experience and extensive knowledge working with a SIEM and performing triage, information gathering and analysis.
- Experience in Security Incident Handling and Incident Management procedures.
- Experience with writing clear and concise technical documents specifically event analysis and incident handling documentation.
- Experience with Intrusion Detection and Prevention Systems.
- Knowledge of computer networking, routing and switching with knowledge of the TCP/IP stack and other protocols.
- Experience with Linux/UNIX and Windows based devices at the System Administrator level.
- Working knowledge of security architectures and devices.
- In-depth knowledge of lateral movement methods, foothold tactics, and data exfiltration techniques.
- Experience with Account Management, Windows Events and Log Management.
- Organizational skills and the ability to work autonomously with attention to detail and processes.
- Excellent communication skills with experience providing incident briefings to peers, management and clients.
- Excellent written skills with experience creating formal incident reports.
- Suitable to obtain Canadian Federal Government SECRET clearance, or the ability to obtain a clearance.

HITACHI
Inspire the Next

We offer:

- Professional environment in cutting-edge technology
- Dynamic work setting in new and modern office
- Employee Referral Bonus
- Group insurance plan
- Team spirit and dedication to service excellence
- Sense of belonging to a global, brand-name organization

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville, QC J7C 5J6 Canada Tel: +1 450-430-8166/ +1 866-430-8166 (toll-free) Fax: +1 450-430-1858
www.hitachi-systems-security.com

HITACHI
Inspire the Next

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville, QC J7C 5J6 Canada Tel: +1 450-430-8166/ +1 866-430-8166 (toll-free) Fax: +1 450-430-1858
www.hitachi-systems-security.com